HTTP Activity vs. User Activity

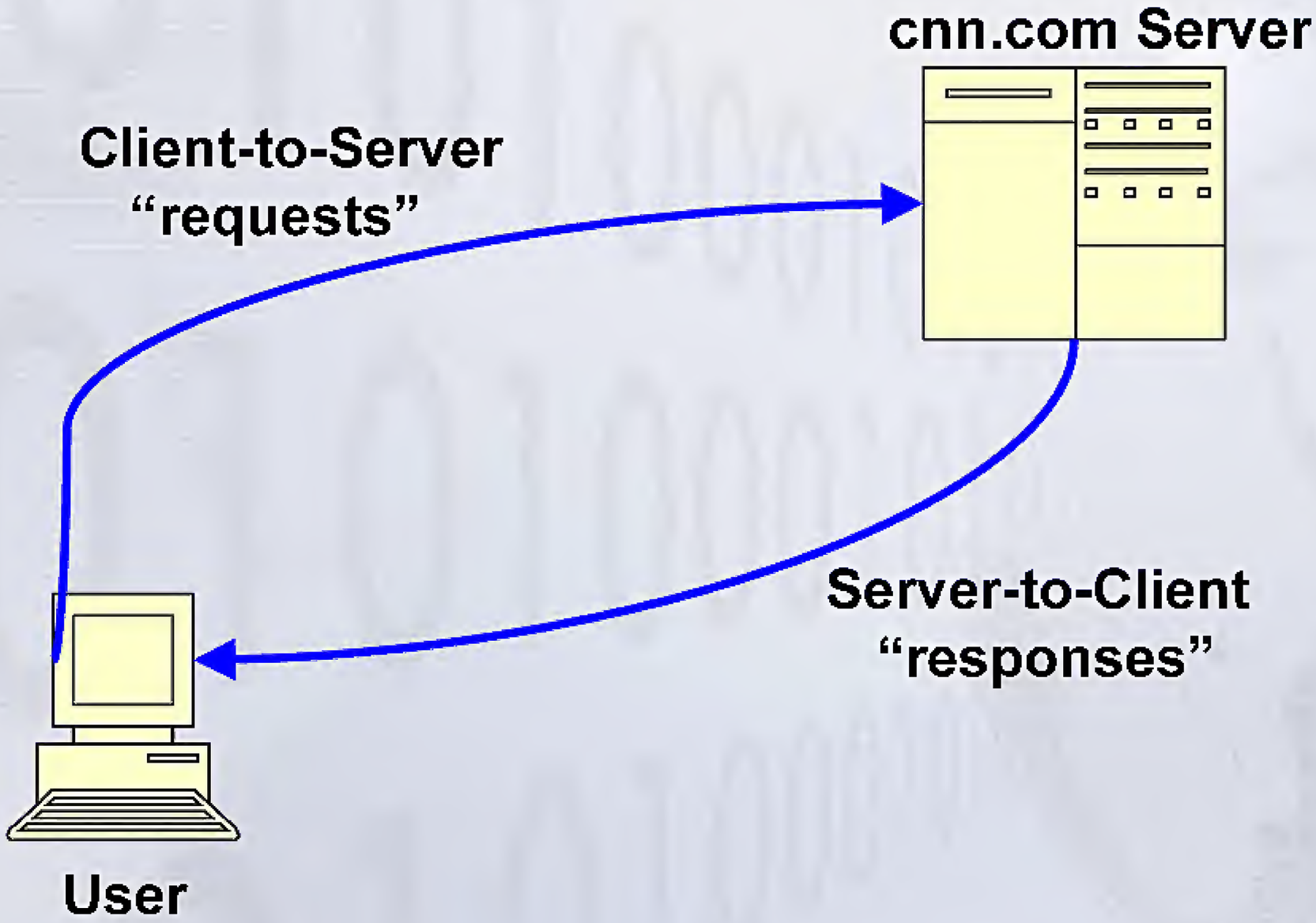
19 June 2009

HTTP Activity

- HTTP Activity is essentially all web-based activity from a user's internet browser (with some exceptions)
- It includes, web-surfing, Internet Searching (like Google), Mapping Website (Google Earth/Maps) etc.

HTTP Activity

- HTTP activity comes in two types:



HTTP Activity Client-to-Server


```
GET /search?tab=urdu&order=sortboth&q=musharraf&start=3&scope=urdu&link=next HTTP/1.1
Accept: */*
Referer: http://search.bbc.co.uk/search?tab=urdu&order=sortboth&q=musharraf&start=2&scope=urdu
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Host: search.bbc.co.uk
Cookie: BBC-UID=b479a5f4ad230a53063d513630203acb22684634a0e0b164c45f96efc054cf950Mozilla%2f4%2e0%20%28co
Cache-Control: max-stale=0
Connection: Keep-Alive
X-BlueCoat-Via: 66808702E9A98546
```

Host	URL Path	URL Args
search.bbc.co.uk	/search	tab=urdu&order=sortboth&q=musharraf&start=3&scope=urdu&link=next

Search Terms	Language	Browser	Via
musharraf	en	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)	66808702E9A98546

Referer
http://search.bbc.co.uk/search?tab=urdu&order=sortboth&q=musharraf&start=2&scope=urdu

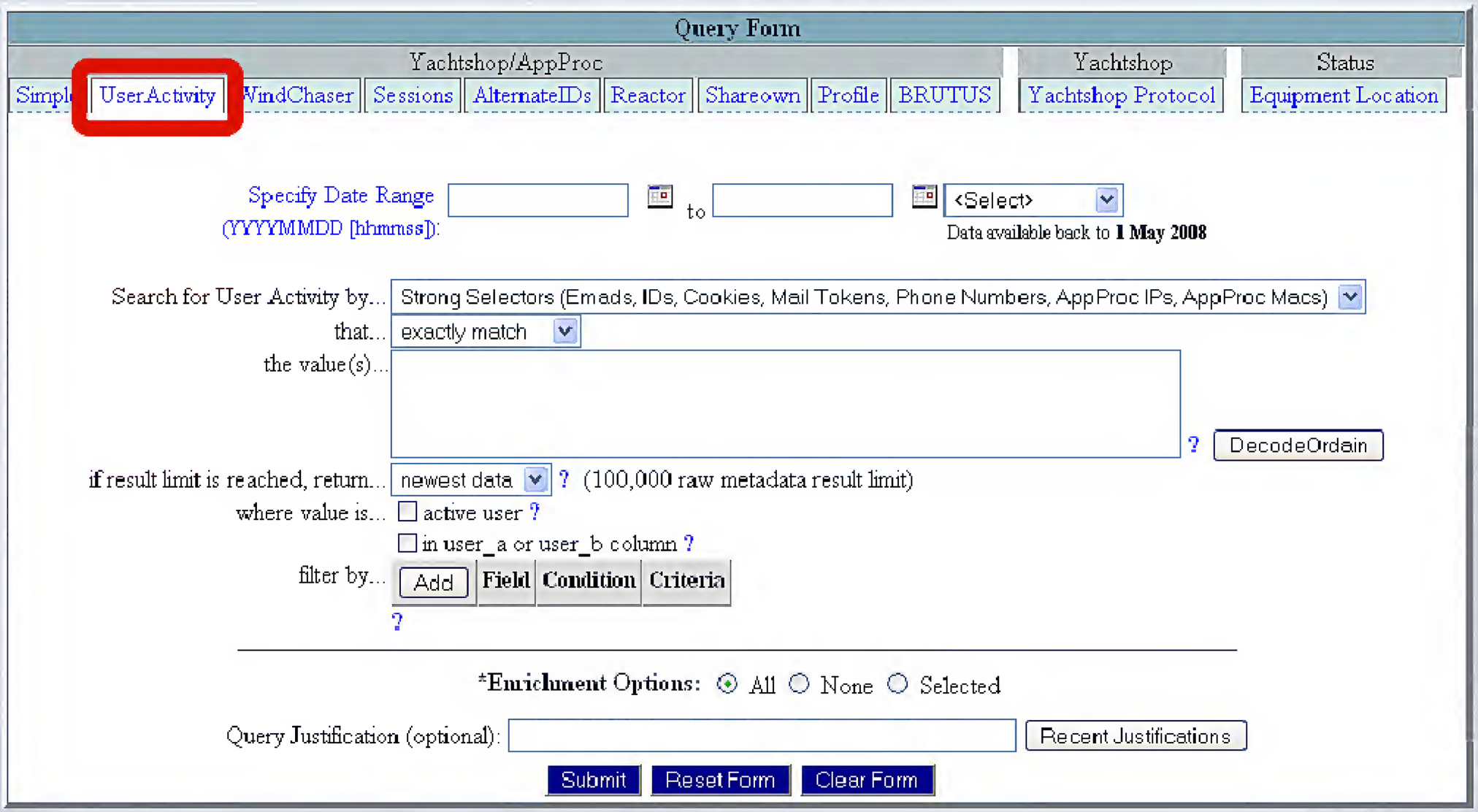
Cookie
BBC-UID=b479a5f4ad230a53063d513630203acb22684634a0e0b164c45f96efc054cf950Mozilla%2f4%2e0%20%28com

User Activity

- User Activity is best described as meta-data from "communication based protocols" like Webmail, Chat, Web Forum, Voip etc. *in which we have protocol processing capabilities like AppProc.*
- It's important to note that there are many applications that fall within this definition in which we do not currently have protocol processing capabilities

User Activity

- Most analysts will probably already be familiar with “User Activity” from MARINA



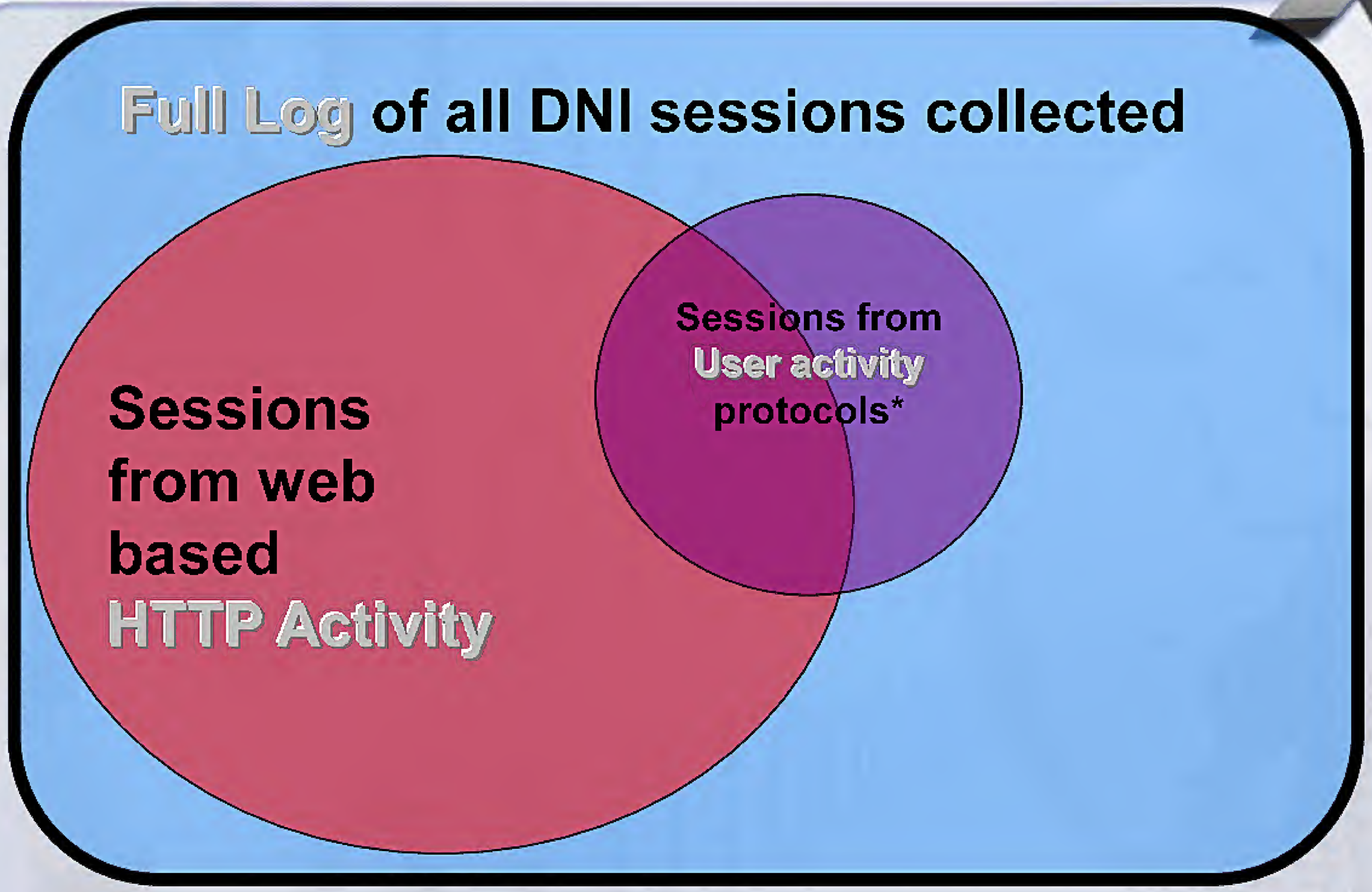
User Activity

- While not an exact duplicate, MARINA and XKS's User Activity share a lot in common
- XKS runs the same software (AppProc/WebProc/StarProc) that is used to break out meta-data for MARINA
- In some cases, it's actually the XKS at the front-end site that is feeding the meta-data to MARINA (the source will be 'XKS')

Overlap

- Since applications like web-mail are web-based, HTTP and User activity will contain information about the same session.
- While HTTP contains information about all web-based sessions, user activity contains information on “user activity protocols” in which we have identified and developed exploitation capabilities

How the Search Forms Fit Together



Examples of traffic

- Webmail (client side)

Datetime	Case Notation	From IP	To IP	From Port	To Port	Protoco	Length
2009-06-17 12:02:27	IRS1014A	85.[redacted] (Iran)	69.[redacted] (United States)	37171	80	TCP	1440

Session | Header (3) | Meta (9)

Formatter: DNI_PRESENTER | Send to: Download Session | Mode: Snippet | Options | Search Content: Enter text to search

TOP SECRET//COMINT//20320108

ID: sess_orig_proc

Type: HTTP-GET | Printer Friendly Version

DNI Display | Raw Data | DNI Format

Services

GET /mc/modules/im/abContacts?mcrumb=RIIDbfi9ijm &.jsrand=98037807 &.rand=2127033459 HTTP/1.0

Accept:	*/*
Accept-Language:	fa
Referer:	http://us.mc575.mail.yahoo.com/mc/showFolder;_ylc=X3oDMTBucmhobGR0BF9TAzM5ODMwMTAyNwRhYwNkZWxNc2dz?mid=1_21857_AERkxELAANvjSi6wUQ7filZa4fY&fid=Inbox&sort=date&order=up&startMid=36&filterBy=
x-requested-with:	XMLHttpRequest
Accept-Encoding:	gzip, deflate
User-Agent:	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727)
Host:	us.mc575.mail.yahoo.com
Cookie:	

MG	d=IvAXlFvaYnFGnmIfzw3zBCVVRe2jUKZLwwyoKSrjxxG0XVYaJhF95dLsZ5C0x1eDlcTcaHS_vpiad9XvB0emj5Rr1 v=1
Y	v=1 n=66k3gh6ns55lf l=ce70cc03_01sqqx/o **(Yahoo login id: [redacted])** p=m2g265i013000000 **(Gender: male, Birth year: [redacted] Postal code: [redacted])** r=hq lg=en-US **(Language/content: English)**

Examples of traffic

- Webmail (server side)

Datetime	Case Notation	From IP	To IP	From Po	To Por	Protoc	Length
2009-06-16 18:23:5	IR1S021D0000000(	69.[redacted] (United State:	91.[redacted] (Iran)	80	60318	tcp	179354

Session | Header (3) | Meta (5) | Attachments (2)

Formatter: DNI_PRESENTER | Send to: Download Session | Mode: Snippet | Options | Search Content: Enter text to search

TOP SECRET//COMINT//20320108

ID: sess_orig_proc

Document Information | Type: HTTP | Printer Friendly Version

DNI Display | Raw Data | DNI Format

HTTP Header Information | Content Type: HTTP/YahooWebmail

Services

UIS Webmail Display YAHOO! MAIL Classic Active user: Unknown

Folder List	
Name	Count
Inbox (1655)	4035
Drafts (5)	5
Sent	831

Message in folder: Inbox

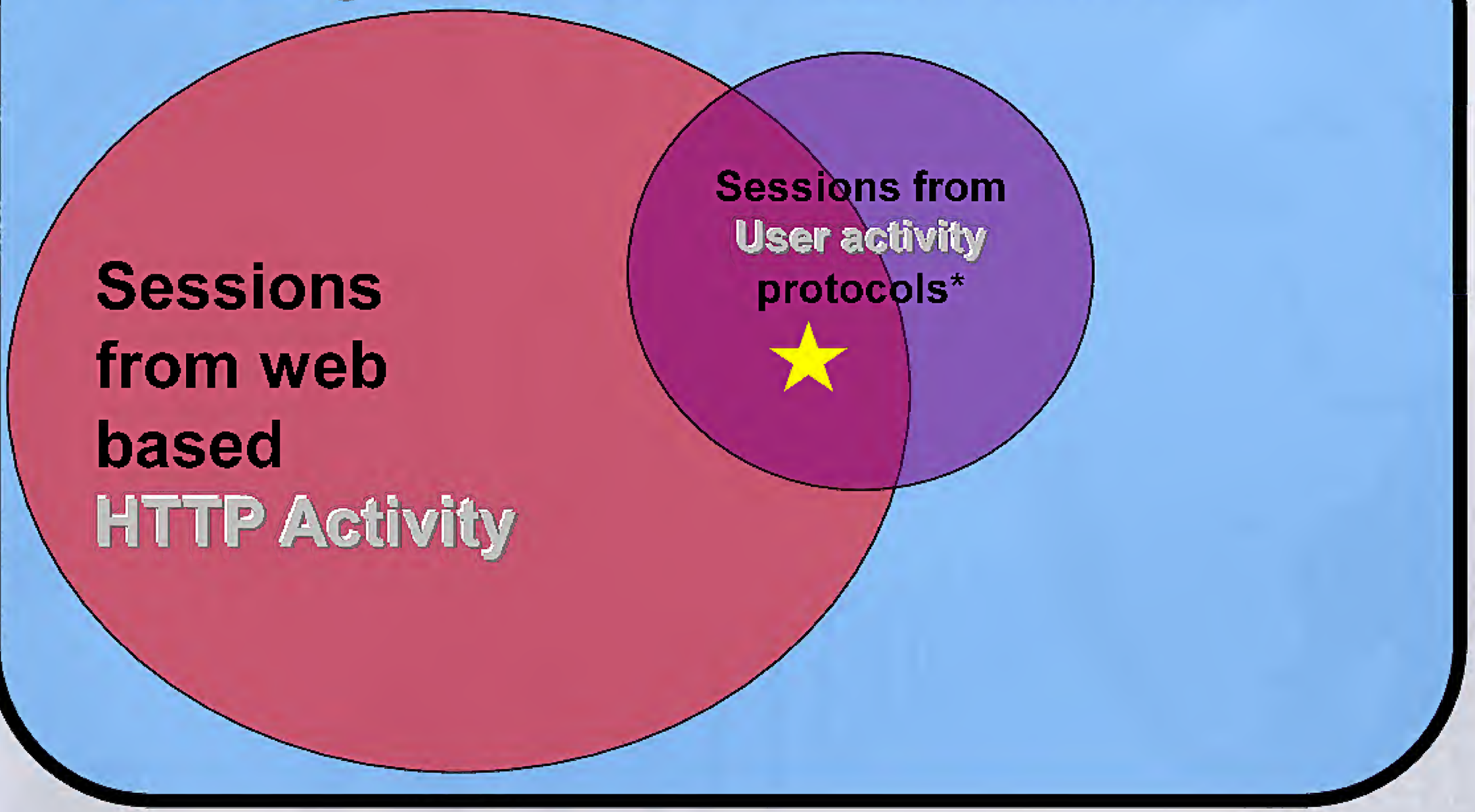
Fwd: Fw: حذف عکس احمدی نژاد...

Tuesday, June 16, 2009 1:14 AM

From:

Yahoo Webmail

Full Log of all DNI sessions collected



Examples of traffic

- MSN Messenger

Datetime	Case Notation	From IP	To IP	From P	To Pc	Proto	Length
2009-06-16 16:1	IRS1014A	89.[redacted] (Iran)	65.[redacted] (United St	51818	1863	TCP	137

Session | Header (3) | Meta (7)

Formatter: DNI_PRESENTER | Send to: Download Session | Mode: Snippet | Options | Search Content:

TOP SECRET//COMINT//20320108

20090616 161707Z [redacted]@yahoo.com<msnpassport> logged in (im) 89.[redacted]

DNI Display | Raw Data | DNI Format

MSN Messenger Message Display | ☑ Display Status Messages | ☐ Show Messages Only | ☐ Reverse

Messages

From	To	Message	Size:
		[redacted]@yahoo.com logging in	

Server Processing Time: 2 ms | Data Load Time: 0 ms | Type: MSN Messenger

Project Manager: [redacted]
Page Publisher: [redacted]
Version: 1.4.0.3
Build Date: Thu Feb 19 13:02:15 GMT 2009

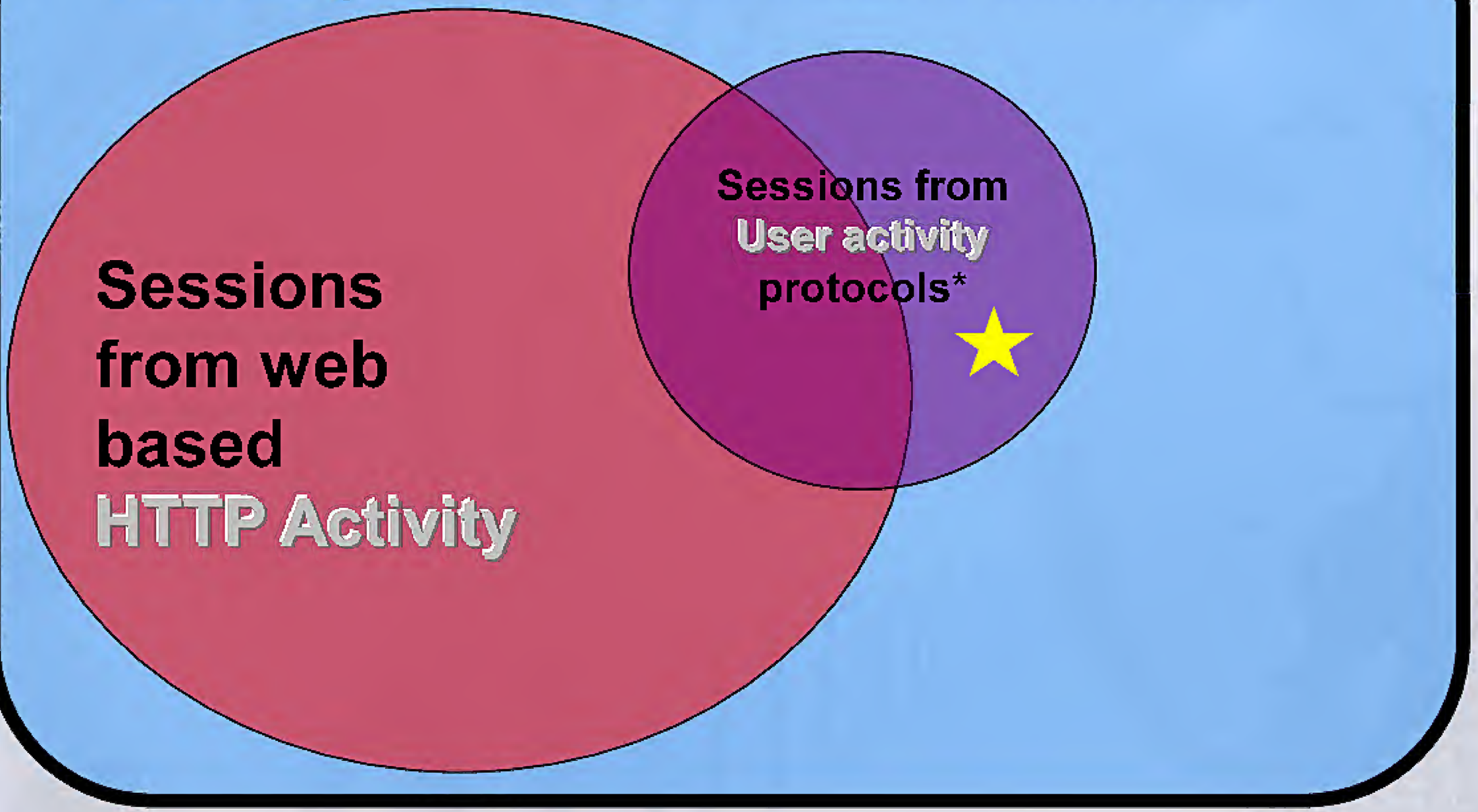
ozone UIS DNI PRESENTER

TOP SECRET//COMINT//20320108

MSN Messenger

KEYSCORE

Full Log of all DNI sessions collected



Examples of traffic

- Skype sessions:

Datetime	Case Notation	From IP	To IP	From Port	To Port	Protocol	Length
2009-06-16 15:25:46	IRS1014B	89.[redacted] (Iran)	89.[redacted] (Switzerland)	14414	13510	UDP	179

Session | Header (3) | Meta (3)

Formatter: DNI_PRESENTER | Send to: Download Session | Mode: Snippet | Options | Search Content: Enter text to search

TOP SECRET//COMINT//20320108

ID: sess_orig_proc

Type: SFF/Binary | Printer Friendly Version

89.[redacted]	has leaker IP	10.0.0.3 c82814cf5ff05776<SkypeNode>
89.[redacted]	seen with machine ID	c82814cf5ff05776<SkypeNode> c82814cf5ff05776<SkypeNode>
[redacted]<SkypeUser>	seen with machine ID	c1695fc7feef159e<SkypeNode> c82814cf5ff05776<SkypeNode>
[redacted]<SkypeUser>	has buddy	[redacted]<SkypeUser> c82814cf5ff05776<SkypeNode>
89.[redacted]	client to server	89.[redacted] c82814cf5ff05776<SkypeNode>
[redacted]<SkypeUser>	logged in (im)	89.[redacted] c82814cf5ff05776<SkypeNode>
[redacted]<SkypeUser>	seen with machine ID	c82814cf5ff05776<SkypeNode> c82814cf5ff05776<SkypeNode>

Project Manager: [redacted]
Page Publisher: [redacted]
Version: 1.4.0.3
Build Date: Thu Feb 19 13:02:15 GMT 2009

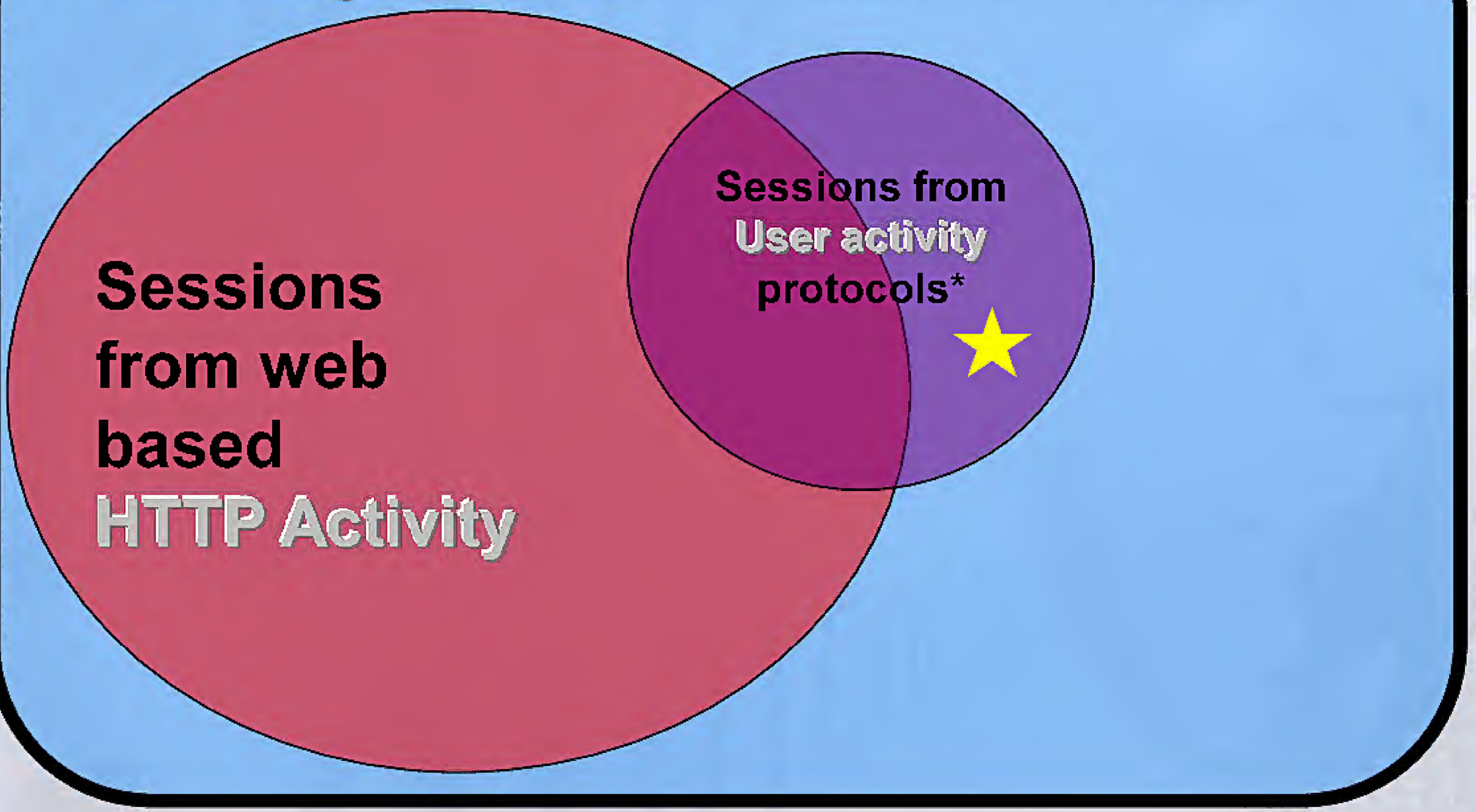
ozone | DNI PRESENTER

TOP SECRET//COMINT//20320108

Skype

KEYSCORE

Full Log of all DNI sessions collected



Example #1

- The typical way to search HTTP Activity is to start with User Activity in MARINA.
- For example, we'll start with this 16 June activity

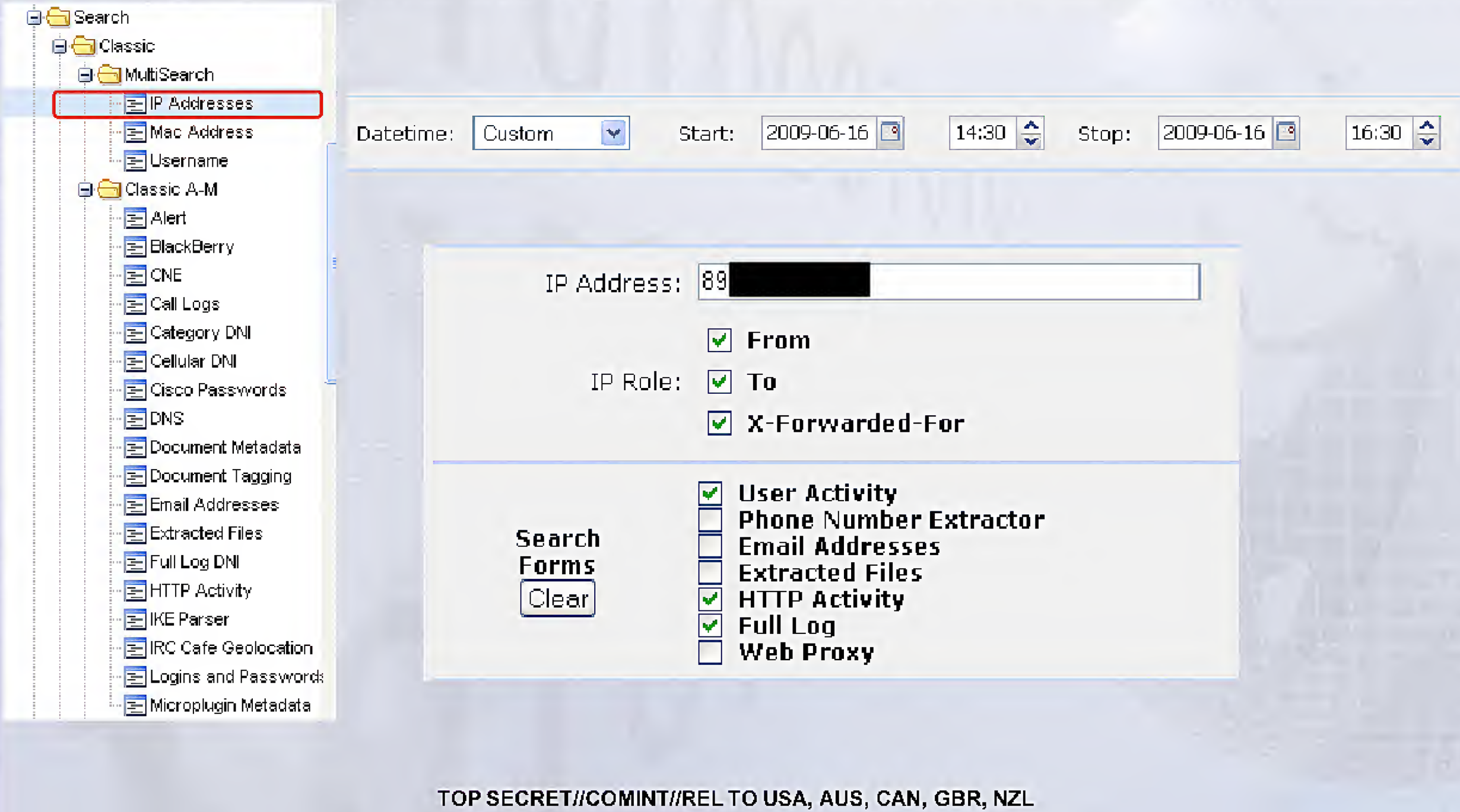
TS ▲	USERID	PHONE	USER_A	*ACTIVITY*	USER_B
20090616 143827Z	[redacted]		<SkypeUser>	logged in (im)	89.[redacted]
20090616 143936Z	[redacted]		<SkypeUser>	logged in (im)	89.[redacted]
20090616 144127Z	[redacted]		<SkypeUser>	logged in (im)	89.[redacted]
20090616 144409Z	[redacted]		<SkypeUser>	logged in (im)	89.[redacted]
20090616 144427Z	[redacted]		<SkypeUser>	logged in (im)	89.[redacted]
20090616 144715Z	[redacted]		<SkypeUser>	logged in (im)	89.[redacted]
20090616 144715Z	[redacted]		<SkypeUser>	logged in (im)	89.[redacted]
20090616 144715Z	[redacted]		<SkypeUser>	logged in (im)	89.[redacted]
20090616 144715Z	[redacted]		<SkypeUser>	logged in (im)	89.[redacted]
20090616 144715Z	[redacted]		<SkypeUser>	logged in (im)	89.[redacted]
20090616 144715Z	[redacted]		<SkypeUser>	logged in (im)	89.[redacted]
20090616 144717Z	[redacted]		<SkypeUser>	logged in (im)	89.[redacted]
20090616 144717Z	[redacted]		<SkypeUser>	logged in (im)	89.[redacted]
20090616 144718Z	[redacted]		<SkypeUser>	logged in (im)	89.[redacted]
20090616 144950Z	[redacted]		<SkypeUser>	logged in (im)	89.[redacted]

Understand what is behind the IP

- Ensure Activity on IP can be associated with Target
- Understand IP usage Dynamic/Static
- Research IP using Foxtrail/NKB
- Is it a Proxy, DVBLAN, Dial-Up, DSL, etc
- Is it Client to Server or Server to Client
- Still not sure? User Activity pull for 5 minute period on Foreign IP

MultiSearch on IP Address

- Let's take what we used last week and do a Multi-Search to discover any web activity around the time the account was active



Example #1

- Note the # of results for each search, compared the 28 MARINA results which was for the same IP address and same time frame

My Recent Results

Help Actions View

Query Name	Query Type	Status	Actions	Num Results	Num DBs
16_june_example	user_activity	finished		0	1 of 1
16_june_example	full_log	finished		3223	1 of 1
16_june_example	http_parser	finished		2626	1 of 1

HTTP Results

- Of interest we see visits to Web Pages like:

http://twitter.com/persiankiwi

http://www.bbc.co.uk/persian/

http://tehranlondon.com/

http://ghalamnews.ir/

http://eshterak-matalbejadid.blogspot.com/2009/06/blog-post_4812.html

web search: #iranelection

google search: میرنا احترامی

HTTP Results

- Notice how all of the HTTP GET requests were going to the same IP address even though they are for different web servers….what's going on here?

Host	To IP	To Port	Count
integratedsearch.twitter.com	38.[redacted]	808	489
www.bbc.co.uk	38.[redacted]	808	126
www.newyorker.com	38.[redacted]	808	57
newsimg.bbc.co.uk	38.[redacted]	808	31
twitter.com	38.[redacted]	808	22
www.facebook.com	38.[redacted]	808	21
static.twitter.com	38.[redacted]	808	12
stats.bbc.co.uk	38.[redacted]	808	12
visualscience.external.bbc.co.uk	38.[redacted]	808	7
news.bbc.co.uk	38.[redacted]	808	6
profile.ak.facebook.com	38.[redacted]	808	5

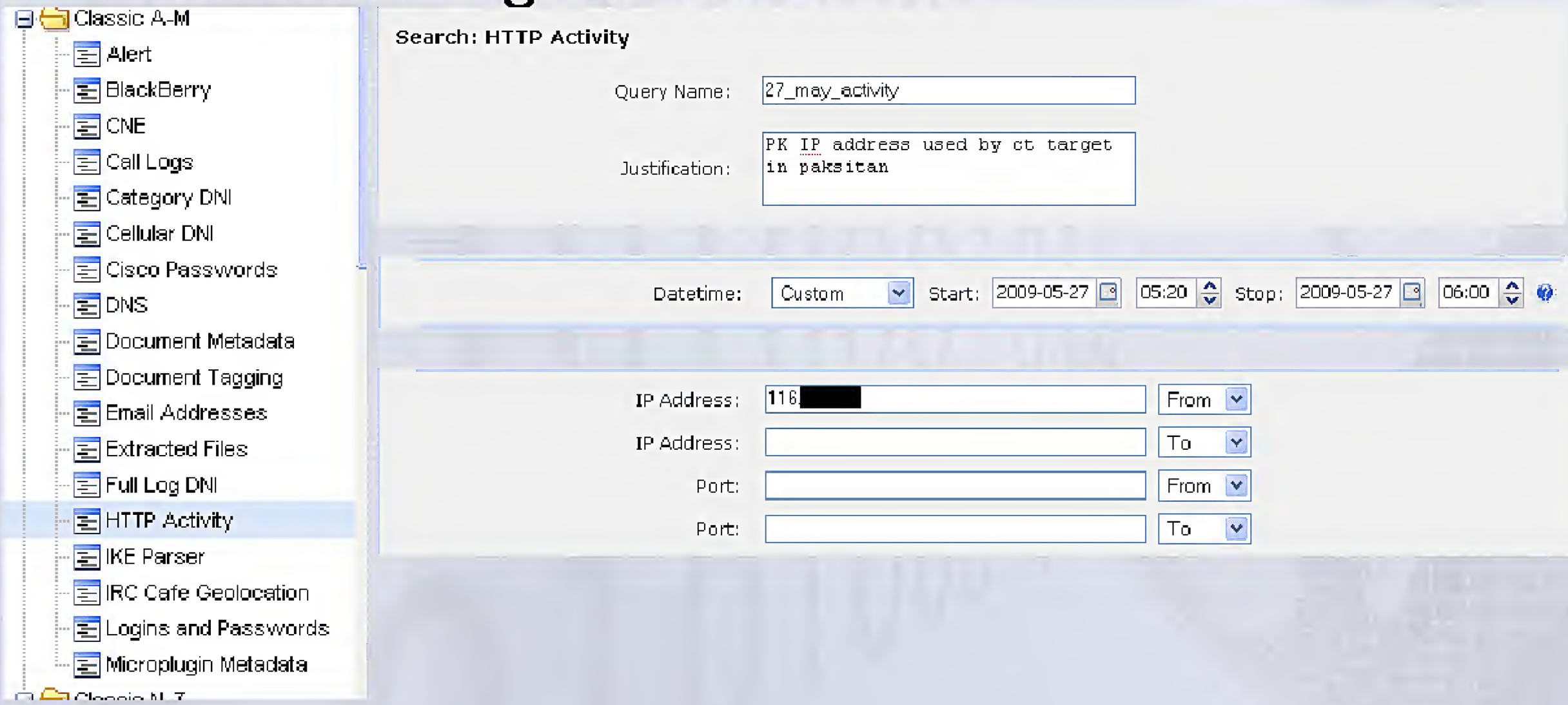
Example #2

- Analysis of 27 May Internet session of PK based target started in MARINA

TS ▲	USERID	PHONE	USER_A	ACTIVITY	USER_B
20090527 052156Z			[redacted]@gmail.com<google>	logged in (email)	116.[redacted]
20090527 052156Z			[redacted]@gmail.com<google>	logged in (email)	116.[redacted]
20090527 052156Z			[redacted]@gmail.com<google>	logged in (email)	116.[redacted]
20090527 052157Z			[redacted]<yahoo>	logged in (email)	116.[redacted]
20090527 052159Z			[redacted]<yahoo>	logged in (email)	116[redacted]
20090527 052236Z			[redacted]<yahoo>	logged in (email)	116.[redacted]
20090527 052236Z			[redacted]<yahoo>	logged in (email)	116.[redacted]
20090527 052236Z			[redacted]<yahoo>	logged in (email)	116.[redacted]
20090527 052236Z			[redacted]<yahoo>	logged in (email)	116.[redacted]
20090527 052236Z			[redacted]<yahoo>	logged in (email)	116.[redacted]

Example #2

- The analyst then did an HTTP activity query to find all web surfing from that IP address within the same rough timeframe.



27 May HTTP Activity

- HTTP meta-data indicated possible Maktoob activity

Datetime	HTTP T	Host	URL Path
2009-05-27 05:22:39	get	cdn.maktoob.com	/newMaktoob/homePage/images/logo.png
2009-05-27 05:22:45	get	cdn.maktoob.com	/newMaktoob/homePage/images/img3.gif
2009-05-27 05:22:45	get	cdn.maktoob.com	/newMaktoob/homePage/images/img4.gif
2009-05-27 05:22:38	get	cdn.maktoob.com	/localization/images/local_toolbar/rit_lctab.gif
2009-05-27 05:22:45	get	cdn.maktoob.com	/newMaktoob/homePage/images/img1.gif
2009-05-27 05:22:39	get	cdn.maktoob.com	/localization/images/local_toolbar/grd_LCtab.gif
2009-05-27 05:22:38	get	cdn.maktoob.com	/localization/images/local_toolbar/flags/ae.gif

Fm C	Fm City (IP)	To C	To City (IP)	Fm IP	To IP
PK	KARACHI	US	HERNDON	116.[redacted]	93.[redacted]
PK	KARACHI	US	HERNDON	116.[redacted]	93.[redacted]
PK	KARACHI	US	HERNDON	116.[redacted]	93.[redacted]
PK	KARACHI	US	HERNDON	116.[redacted]	93.[redacted]
PK	KARACHI	US	HERNDON	116.[redacted]	93.[redacted]
PK	KARACHI	US	HERNDON	116.[redacted]	93.[redacted]
PK	KARACHI	US	HERNDON	116.[redacted]	93.[redacted]

27 May MARINA results

- MARINA didn't show any Maktoob User:

TS ▲	USERID	PHONE	USER_A	ACTIVITY	USER_B
20090527 052156Z			[redacted]@gmail.com<google>	logged in (email)	116.[redacted]
20090527 052156Z			[redacted]@gmail.com<google>	logged in (email)	116.[redacted]
20090527 052156Z			[redacted]@gmail.com<google>	logged in (email)	116.[redacted]
20090527 052157Z			[redacted]<yahoo>	logged in (email)	116.[redacted]
20090527 052159Z			[redacted]<yahoo>	logged in (email)	116.[redacted]
20090527 052236Z			[redacted]<yahoo>	logged in (email)	116.[redacted]
20090527 052236Z			[redacted]<yahoo>	logged in (email)	116.[redacted]
20090527 052236Z			[redacted]<yahoo>	logged in (email)	116.[redacted]
20090527 052236Z			[redacted]<yahoo>	logged in (email)	116.[redacted]
20090527 052236Z			[redacted]<yahoo>	logged in (email)	116.[redacted]

27 May User Activity Results

- XKS's User Activity also didn't show any Maktoob activity

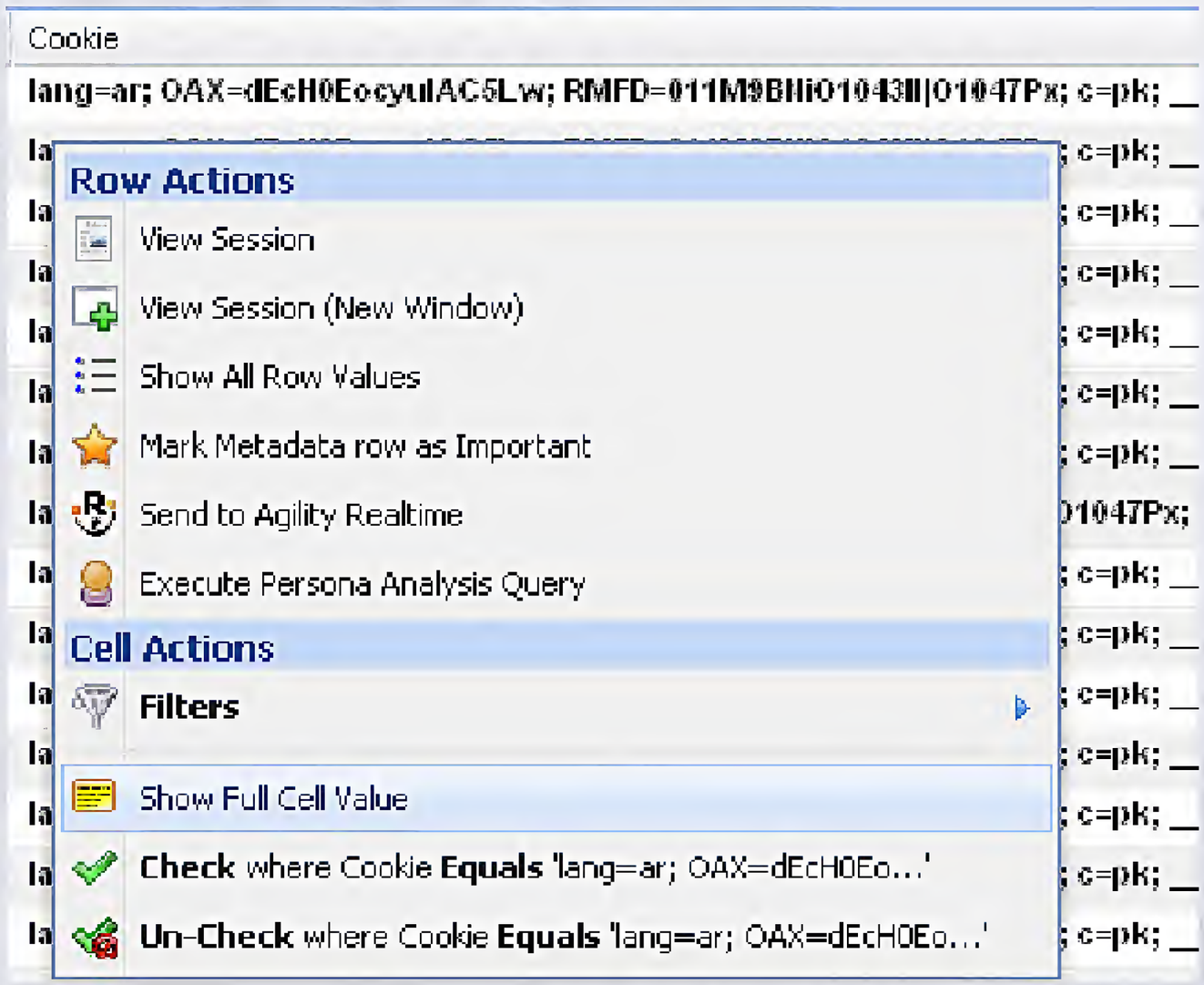
Datetime End	Search Value	Realm	Attribute Type	Attribute Value	Activity
2009-05-27 05:23:58	[redacted]@yahoo	yahoo	B_cookie	bsgamv5517ssv	login_webmail
2009-05-27 05:23:58	[redacted]@yahoo	yahoo	B_cookie	bsgamv5517ssv	login_webmail
2009-05-27 05:23:58	[redacted]@yahoo	yahoo	B_cookie	bsgamv5517ssv	login_webmail
2009-05-27 05:23:58	[redacted]@yahoo	yahoo	B_cookie	bsgamv5517ssv	login_webmail
2009-05-27 05:39:07	[redacted]@yahoo	yahoo	B_cookie	bsgamv5517ssv	login_webmail

27 May HTTP Activity

- Was it just a visit to the Maktoob home page or was there an actual web-mail log-in?
- In most cases “active user” and “previous user” information from web-mail protocols comes from the cookie field.
- XKS HTTP Activity breaks out the entire cookie field, even if protocol analysis doesn’t know what each part means

27 May HTTP Activity

- Look at the full cell value:



27 May HTTP Activity

- By looking at the full cookie, the analyst noticed what appeared to be the target's username ([redacted]):

lang=ar; OAX=dEcH0EocyuIAC5Lw; RMFD=011M9BNiO1043II|O1047Px; c=pk; __ http://www.makt

Cookie

lang=ar; OAX=dEcH0EocyuIAC5Lw; RMFD=011M9BNiO1043II|O1047Px; c=pk;
__utma=206054159.4027773062198129700.1243400938.1243400938.1243401768.2;
__utmb=206054159.1.10.1243401768;
__utmz=206054159.1243400938.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none);
str_tab=sport,news,jokesNew,undefined; MKLLD=[redacted]%22%2C%221243401282;
RMAM=01cen16_1060.4aD066GG|; __utmc=206054159

27 May HTTP Activity

- The content also shows the cookie value:

GET /localization/js/localization.utf-8.js/2009/5/26/8999991 HTTP/1.1	
Accept:	*/*
Referer:	http://web14.maktoob.com/mail2.newlogin/compose432.php?nm=956880045
Accept-Language:	en-us
Accept-Encoding:	gzip, deflate
User-Agent:	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Host:	cdn.maktoob.com
Connection:	Keep-Alive
Cookie:	lang=ar OAX=dEcH0EocyuIAC5Lw RMFD=011M9BNiO1043jt|O1043Il|O1047Px c=pk __utma=206054159.4027773062198129700.1243400938.1243400938.1243401768.2 __utmb=206054159.1.10.1243401768 __utmz=206054159.1243400938.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none) str_tab=sport,news,jokesNew,undefined MKLLD=[redacted]"1243402079 RMAM=01cen16_1060.4aD066GG| wlm_utf-8=0,[redacted] wlm_windows-1256=0,[redacted] __utmc=206054159 MKTID=JDhdVmJ8RRc4fWlFOAZScT81eTcscE97EyoMGlVjeA4sDAdWPzMWQk0LKm5acjxNBjMxN. logged=1

27 May Maktoob Activity

- Why wasn't this activity in MARINA or XKS's User Activity (both fed by AppProc)?
- Because Protocol Exploitation hadn't identified this particular Maktoob service
- Since it hadn't been identified, AppProc could not produce meta-data and DECODEORDAIN was not producing permutations for strong selection

27 May Maktoob Activity

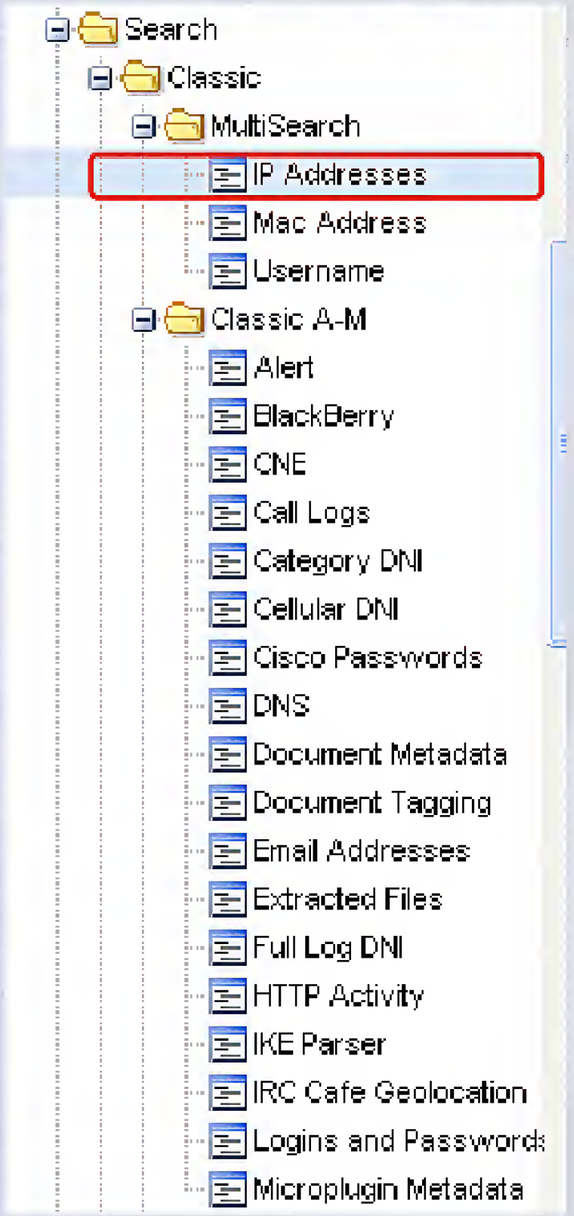
- In this particular case, analysts from Protocol Exploitation were able to determine that the MKLLD= cookie was identifying the “previous user” but not the “active user”

Moral of the story

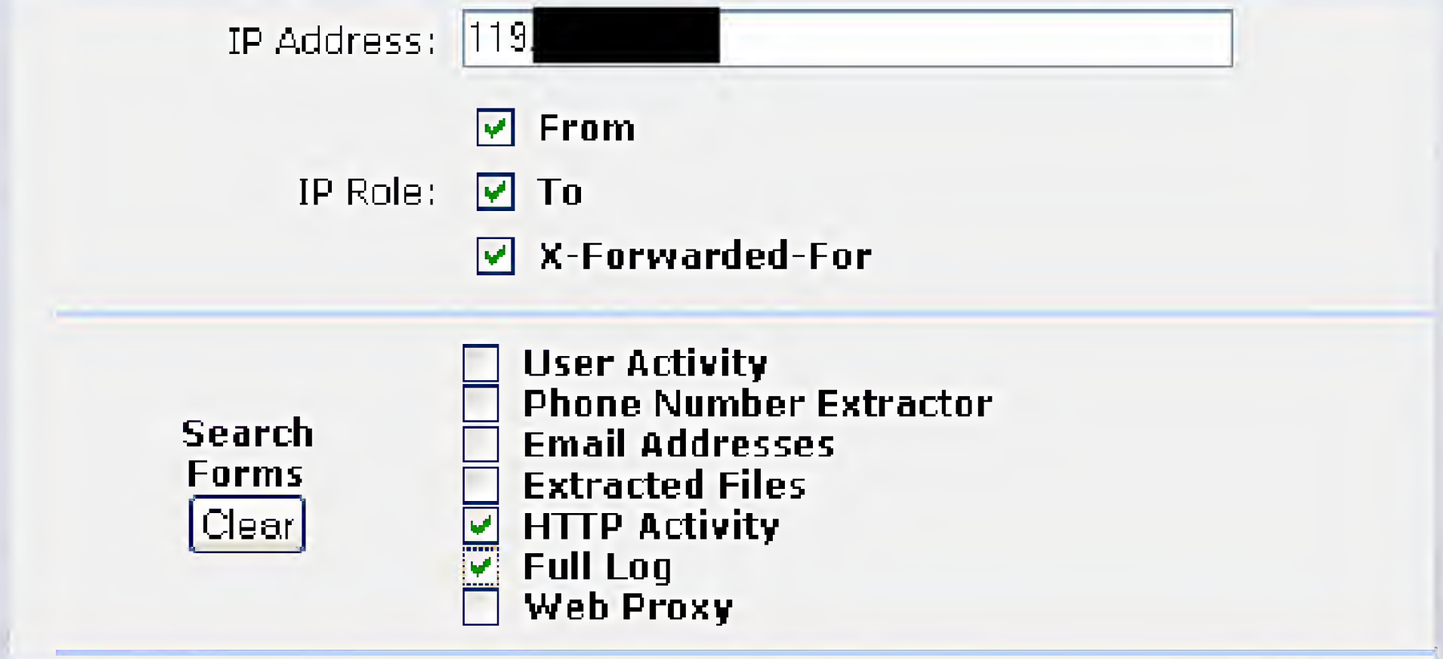
- Internet applications are dynamic, and protocol analysts are not able to identify and build capabilities to exploit every known application
- It's important that target analysts use tools like XKS to aggressively develop their target to uncover applications that are previously unidentified or are not currently being processed properly

Moral of the story

- The Multi-Search page gives you the ability to search full log and HTTP activity based on an IP address at the same time



Simply enter in an IP address, choose any or all "roles" (ie. from/to/xff) and then choose what search forms you want.



Who to contact

- If you discover examples that don't seem to be processing correctly, don't hesitate to contact the experts at traffichelp@nsa.ic.gov